PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04L 9/32

A1

(11) International Publication Number: WO 97/39553

(43) International Publication Date: 23 October 1997 (23.10.97)

(21) International Application Number: PCT/US97/04025

(22) International Filing Date: 14 March 1997 (14.03.97)

(30) Priority Data:
08/634,068 17 April 1996 (17.04.96) US

(71) Applicant (*for all designated States except US*): INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

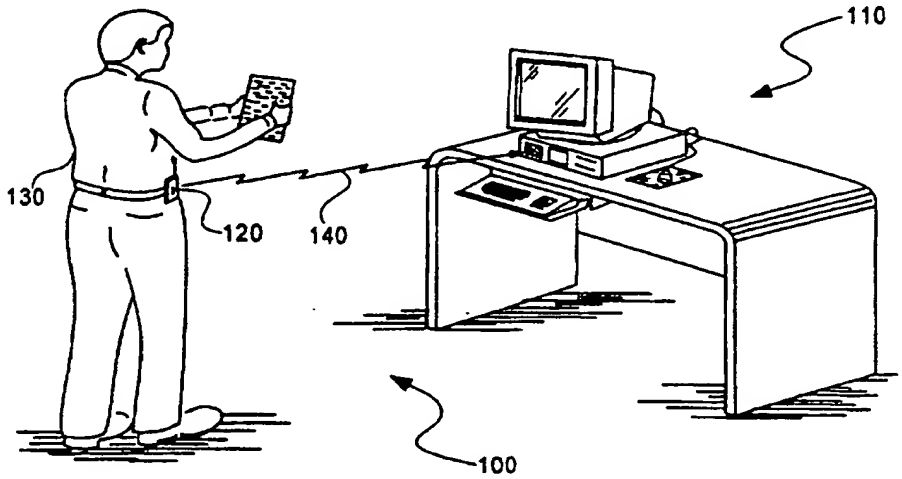
(72) Inventors; and
(75) Inventors/Applicants (*for US only*): DAVIS, Derek, L. [US/US]; 4509 E. Desert Trumpet Road, Phoenix, AZ 85044 (US). SMITH, Lionel [US/US]; 23412 Via del Arroyo, Queen Creek, AZ 85242 (US).

(74) Agents: TAYLOR, Edwin, H. et al.; Blakely, Sokoloff, Taylor & Zafman L.L.P., 1279 Oakmead Parkway, Sunnyvale, CA 94086 (US).

(81) Designated States: AL, AM, AT, AT (Utility model), AU (Petty patent), AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: AN AUTHENTICATION SYSTEM BASED ON PERIODIC CHALLENGE/RESPONSE PROTOCOL



(57) Abstract

A wireless authentication system to control an operating state of a node such as a computer, door control mechanism or any multistate product based on the proximity of an authorized user to the node. The wireless authentication system comprises a security device implemented within the node (110) and a user authentication token ("token") in possession of the authorized user. A Challenge/Response protocol (140) is configured between the security device and the token (120). The first successful Challenge/Response message exchange between the security device and the token (120) places the node (110) in an operational state allowing the authorized user access to the contents and/or networked resources of the node (110). Later Challenge/Response message exchanges are set to occur periodically to check whether the authorized user possessing the token has left the node (110) unattended thereby causing the node (110) to be placed in a non-operational state.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav	TM	Turkmenistan
BF	Burkina Faso	GR	Greece		Republic of Macedonia	TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's	NZ	New Zealand		
CM	Cameroon		Republic of Korea	PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

AN AUTHENTICATION SYSTEM BASED ON PERIODIC CHALLENGE/RESPONSE PROTOCOL

CROSS-REFERENCES TO RELATED APPLICATIONS

The named inventor of the present application has filed a number of co-pending United States Patent Applications entitled "Apparatus and Method for Providing Secured Communications" (Application No. 08/578,177), "Secured Method for Providing Secured Communications" (Application No. 08/538,869), "Method For Providing A Roving Software License In A Hardware Agent-Based System" (Application No. 08/472,951), "Key Cache Security System" (Application No. 08/365,347), and "Apparatus and Method for a Vetted Field Upgrade" (Application No. 08/316,211) and issued U.S. Patent entitled "Roving Software License For A Hardware Agent" (U.S. Patent No. 5,473,692). These applications are owned by the same assignee of the present Application.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to data security. More particularly, the present invention relates to a wireless authentication system which mitigates the likelihood of unauthorized use of an electronic device through periodic challenge/response messages.

2. Description of Art Related to the Invention

As personal computers ("PCs") become more prevalent in businesses throughout the world, it is becoming increasingly important to provide security to prevent their unauthorized use.

Already, there exist a number of authentication systems which provide marginally effective security of one's personal computer. For example, one well-known type of conventional authentication system is a "password-based" system in which a person is allowed access to the contents of and resources networked to a personal computer by correctly typing in a previously chosen password. However, password-based systems are susceptible to (i) software which can be used to capture the person's password and to (ii) common "human" mistakes such as confiding one's password to another or using the same password for a long period of time. Moreover, password-based systems do not provide any mechanism for mitigating the risk of unauthorized use of one's personal computer in those situations where the user fails to turn-off his or her personal computer before leaving work or has to leave his or her office for a moment (e.g., lunch, attend a meeting, etc.) but leaves his or her personal computer running i.e., in an operational state.

Another example is a password protected screen saver which automatically turns off one's computer if it is not used for a predetermined period of time. This authentication system is usually disruptive to the user because its state is dependent on whether or not the user is using the computer, not the proximity of the user to the computer. Thus, if the user is on the phone for a while, the computer may be mistakenly turned off requiring the user to log-in again. Thus, users commonly set the "time-out" of the screen saver for a long duration which defeats its objective to protect the contents of the computer when the user has left his or her office without turning off the computer.

Another marginally effective authentication system is a "card-based" system in which a "smartcard" card being an integrated circuit carried in a credit card form factor, PCMCIA card or magnetic stripped card (hereinafter generally referred to as "token cards") is used to gain physical and/or electrical access to the personal computer. Normally, token cards may be either inserted into a designated card slot of the personal computer, placed in physical contact with a reading device coupled to the computer or placed in an area where the personal computer resides (e.g., an office, laboratory and the like). These token cards are used to verify that the person in possession of the card is in fact authorized to use the personal computer. Depending on the type of token card, such verification is accomplished by the token card responding to a request (i.e., "Challenge message") for information by providing a "token" (i.e. code), normally a random number although it may be static, in response to the challenge issued by the personal computer. In the case of a more sophisticated token card, this request will be in the form of a random "challenge" which the token card must first process in order to provide the correct "response". Although this type of authentication system arguably provides greater security than the password-based system, it still does not solve the problem where the user accesses his or her personal computer and leaves the personal computer unattended for some duration without removing the card or disabling the personal computer during his or her absence.

Hence, it is desirable to develop a wireless authentication system which does not require a physical connection to the personal computer, thereby mitigating the chances of mistakenly leaving one's token card within or in proximity of one's computer. While there now exist some authentication systems in the marketplace such as those provided by Security Dynamics, Inc. of Cambridge, Massachusetts and Digital Pathways of Mountain View, California, their systems do not utilize periodic Challenge/Response protocol to ascertain whether the authorized user of the personal computer has left his or her personal computer unattended for a predetermined period of time.

SUMMARY OF THE INVENTION

A wireless authentication system to control an operating state of a first node (e.g., computer) based on the proximity of an authorized user to the first node. The wireless authentication system comprises a security device implemented within the first node and a user authentication token in possession of the authorized user (e.g., worn, carried, etc.). The security device generates a Challenge message and transmits the same to the token. In response, the token generates and transmits a Response message to the security device if the token is within a predetermined distance from the security device. Thereafter, the authorized user can access the first node because it is in an operational state.

Subsequently, the security device generates and transmits other Challenge messages at selected intervals to check whether the authorized user normally wearing the token has left the first node unattended. If the token responds correctly indicating that the token is still proximate to the first node, the first node is maintained in its operational state. Otherwise, the first node enters into a non-operational state disallowing further access thereto.

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the present invention will become apparent from the following detailed description of the present invention in which:

Figure 1 is a perspective view of the wireless authentication system comprising a personal computer periodically producing a Challenge message to query the proximity of the user and his or her token as well as the token producing a Response message in response to the Challenge message.

Figure 2 is a block diagram of the general architecture of the personal computer of Figure 1.

Figure 3 is a block diagram of an illustrative embodiment of the security device employed within a node as shown in Figure 2.

Figure 4 is a block diagram of an illustrative embodiment of the token of Figure 1.

Figure 5 is a flowchart illustrating the procedural steps undertaken by the wireless authentication system in protecting the integrity of the contents and networked resources of the node through periodic Challenge and Response messages.

Figures 6A-6C are block diagrams of three illustrative embodiments of the Challenge/Response protocol.

Figure 7 is an illustrative embodiment of the operations for configuring the token to provide security against the unauthorized access of the node.

DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention relates to a wireless authentication system which provides and maintains a node in an operational state only when, through periodic bi-directional communications, it ascertains whether an individual wearing a user authentication token is within a predetermined (approximate) distance from the node. In the following description, numerous specific details are set forth but it is appreciated to one skilled in the art that these exact details are not required to practice the present invention. Likewise, certain well-known components, devices and method steps are not set forth in detail to avoid unnecessarily obscuring the present invention.

Herein, certain well-known terminology is generally defined below. For example, a "message" is generally defined as information (e.g., data, address, encrypted keys and any other information) being transferred in a sequence of one or more cycles. Two common types of messages are a "Challenge" message and a "Response" message collectively authenticating the user of the node and his or her whereabouts. A "key" is an encoding and/or decoding parameter used by cryptographic algorithms such as Rivest, Shamir and Adleman ("RSA") which use public and private key pairs and Data Encryption Algorithm ("DES") which use a secret key shared in confidence between two parties. A "digital certificate" is defined as any digital information (e.g., a public key) encrypted of a private key of a widely known trusted authority (e.g., bank, governmental entity, trade association, equipment manufacturer, company security, system administration, etc.) to securely transmit the digital information between two electronic devices.

Referring to Figure 1, an illustrative embodiment of the wireless authentication system of the present invention is shown. The wireless authentication system 100 features a security device (not shown) implemented within a node (e.g., a personal computer) 110 and a user authentication token ("token") 120 worn by an authorized user 130. The token 120 may be constructed in any form, preferably a form that is not too obtrusive to carry or wear. Examples of forms that can be used by the tokens include, but are not limited to pagers or identification badges. The function may also be implemented in another device with an alternative purpose such as a cellular telephone. The personal computer 110 periodically attempts to establish a communication link 140, represented by dotted lines, with the token 120 through infra-red ("IR") transmissions or through any other medium that does not require physical connection (e.g., radio frequency "RF" signals in which the personal computer 110 may require an antenna). The communication link 140 may be established and maintained only when the token 120 is within a predetermined distance (e.g., within 20 feet) from the personal computer 110. It is contemplated that although the wireless authentication system is being described with a personal computer, it could be implemented to secure any node being an electronic product such as a peripheral to the computer (printer, mass storage device, etc.), door locking mechanisms (i.e., garage door opener, electronic door locks) and the like.

Upon establishing the communication link 140, information is exchanged, normally in an encrypted format in at least one direction, between the security device (not shown) and the token 120. Upon the security device determining that the token 120 responded correctly, the user 130 is granted access to the contents (i.e., data, applications and other information stored thereon) of the personal computer 110 as well as its networked resources.

It is contemplated that the wireless authentication system 100 may be utilized with another authentication system (password-based system, card-based system, etc.) to prevent the personal computer 110 from being mistakenly accessed in certain situations. One situation is where the authorized user 130 wearing the token 120 is walking by the personal computer 110 within the predetermined distance without any intention of using the personal computer 110.

Referring now to Figure 2, an embodiment of the personal computer 110 featuring the security device of the authentication system is illustrated. The personal computer 110 includes a first bus 200 enabling information to be communicated between a security device 210, a wireless interface 215 and a plurality of subsystems including a processor subsystem 220, a memory subsystem 240 and an input/output ("I/O") subsystem 260. The details of the security device 210 are discussed in Figure 3 and the wireless interface 215 is a conventional interface which is constructed to transmit and receive messages in an "IR" or perhaps "RF" format.

As further shown in Figure 2, the processor subsystem 220 includes a host processor 225 illustrated as a single processor but may be employed as multiple processors within the personal computer 110. It is contemplated that the security device 210 is represented as a co-processor but the authentication operations could be performed by the host processor 225, provided there is no concern about virus attack or removal of the chassis of the personal computer to monitor its bus signals. However, since the host processor is an open platform architecture, implementation of the security device 210 itself or its functionality within the host processor 225 would require isolation of the authentication operations from normal operations of the host processor 225.

The memory subsystem 240 includes a memory controller 245 which is coupled to the first bus 200. The memory controller 245 controls the access to at least one memory device 250 such as dynamic random access memory ("DRAM"), read only memory ("ROM"), video random access memory ("VRAM") and the like. The memory device 250 stores data, instructions and other information for use by the host processor 225.

The I/O subsystem 260 includes an I/O controller 265 which is coupled to both the first bus 200 and a second bus 270 (e.g., a Peripheral Component Interconnect "PCI" bus, Industry Standard Architecture "ISA" bus and the like). The I/O controller 265 provides a communication path to allow devices connected to the first bus 200 or the second bus 270 to exchange information. The second bus 270 allows information to be transferred from or to at least one peripheral device including, but not limited to a display device 275 (e.g., cathode ray tube, liquid crystal display, etc.); an alphanumeric input device 276 (e.g., an alphanumeric keyboard, etc.) for communicating information (address, data and control) to the host processor 225; a cursor control device 277 (e.g., a mouse, trackball, joystick, touchpad, etc.); a mass data storage device 278 (e.g., magnetic tapes, hard disk drive, floppy disk drive, etc.); an information transceiver device 279 (fax machine, modem, etc.) for transmitting information from the personal computer 110 to another remotely located device and for receiving information therefrom; and a hard copy device 280 (e.g., plotter, printer, etc.) for providing a tangible, visual representation of the information. It is contemplated that the personal computer shown in Figure 2 may employ some or all of these devices or different devices than those illustrated. For example, the security device 210 could be coupled to the second bus 270 instead of the first bus 200, a local bus (not shown) within the host processor 225 or may be adapted to any bus line coupling any of the peripheral devices such as the mass storage device 278.

Alternatively, the security device could be utilized for access control purposes outside the computer field such as in the automatic field, home and business security field. It is contemplated that the security device and token combination could be used to authenticate the holder of the token before granting access to a node of transportation (car, bus, farm equipment, etc.) garage, and home or office or any other node by implementing the security device in that node such as within a door control mechanism (e.g., garage door opener, electronic locks, etc.) and the like.

Referring to Figure 3, one embodiment of the security device 210 is shown. The security device 210 includes a processing unit 211 and a memory unit 212. The processing unit 211 may be a co-processor, micro-controller or any other device having processing capabilities. The memory unit 212 preferably is made of non-volatile memory which is able to contain cryptographic algorithms as well as cryptographic keys (e.g., public key(s) of various tokens, a public key of the widely known trusted authority, a unique public/private key pair, a DES key, etc.). In this embodiment, both the processing unit 211 and the memory unit 212 are implemented in a single integrated circuit package 213 to mitigate the risk of tampering although they may be separately packaged and hardwired together. The security device 210 may include an interface 214 coupling the processor unit 211 to the first bus.

Referring now to Figure 4, one embodiment of the token 120 is shown. The token 120 comprises a wireless interface 300 to exchange messages, namely Challenge and Response messages with the personal computer or any node. These messages may follow an IR or RF transmission protocol although other types of transmission protocols may be used. The wireless interface 300 is coupled to a processor 310 and a memory element 320, both of which are preferably integrated into one integrated circuit package 325 to reduce vulnerability to physical tampering. The memory element 320 has non-volatile characteristics (either as true non-volatile memory or as RAM with a "permanent" power source such as a battery) and is preferably configured to contain its unique public and private key pair and perhaps a digital certificate to allow the token 120 to securely transmit its public key "PUT" to the security device in the event that the security device is not configured at manufacture with various public keys of tokens whose users are allowed access to the personal computer or its controlling node. It is an option for the token 120 to provide an on-board power source 330 (e.g., a battery) to possibly supply power to components within the token 120 for operational purposes as well as to possibly service the memory element 320 if needed. For some protocol implementations, inclusion of a random number generator may be desirable (particularly where the token is also used to authenticate the personal computer).

Referring to Figure 5, the operational steps performed by the wireless authentication system in periodically exchanging Challenge and Response messages between a node (e.g., computer, locking mechanism for car doors, home or office door entry, etc.) and the token is illustrated. In this embodiment, the node prompts a user for a password but continues to deny access to its contents and networked resources (Steps 400-405). Upon the user entering his or her password, the node determines whether the password is correct (Step 410). If the password is incorrect, the node prompts the user to re-enter the password. Of course, the node may be configured to allow only one or more tries to enter the password before precluding access to the node without assistance by security (such as a corporate security officer) or imposing a time-delay before one can attempt to try to access the node.

Alternatively, if the password is correct, the node, namely the security device, generates a Challenge message and transmits the Challenge message covering a predetermined distal range from the node (Step 415). Thereafter, it awaits a Response message from the token and its verification before allowing the user access to the content stored on the node or its networked resources (Step 420). If no Response message is received after a prescribed period of time, access is denied (Step 425). Otherwise, upon receiving the Response message, the node verifies whether the Response message is correct (Step 430). If the Response message is incorrect, the user is denied access to the node by any conventional manner such as by displaying a screen-obscuring image, refusing further input from the keyboard, mouse, etc., suspending further I/O to and from the node or suspending any network connections for a computer representing the node. If the Response message is correct, the user is provided access to the node and a timing circuit integrated in the node is set to signal when the node is to generate another Challenge message and undergo another Challenge/Response session (Steps 435-445). This ensures that the node will periodically require authentication and implicitly the proximity of the user from the node before maintaining it in its operational state or placing it in a non-operational state.

The periodic Challenge/Response message may be performed in a number of ways as shown in Figures 6A-6C. These are shown purely for clarification; other means of authentication may be used without deviating from the spirit of this invention. For example, the node, namely the security device 210, may generate a random number ("RN") 500 and transmit RN 500 in a non-encrypted format as a Challenge message to the token 120. Upon receiving the Challenge message, the token 120 encrypts RN 500 with its private key "PRT", forming a Response message 505 and returns the Response message 505 back to the security device 210. Thereafter, the security device 210 decrypts the Response message 505 with a public key of the token "PUT" and checks to verify that the random number received ("RN_{rec}") 510 is equivalent to RN 500.

Another example is that the security device 210 may produce a Challenge message 525 by generating a random number "RN" 520 and encrypting RN 520 with the token's public key "PUT" stored within the security device 210. Thereafter, the Challenge message 525 is transmitted to the token 120. Upon receiving the Challenge message 525, the token 120 decrypts the Challenge message 525 with its private key "PRT" to retrieve the random number "RN_{trmt}" 530. Thereafter, RN_{trmt} 530 is transmitted back to the security device 210 and compared with RN 520 previously transmitted to determine if they are equivalent. If so, the user is provided access to the data stored within the node and if not, the user is prevented such access.

Another illustrative example is shown in Figure 6C where the security device 210 is not designed to store any public keys associated with authorized tokens. As a result, a digital certificate is required as shown. The security device 210 transmits a random number ("RN") 540 to the token 120. The token 120 receives RN 540 and encrypts RN 540 with the private key of the token "PRT" to produce an encrypted random number "RN_{prt}" 545 as part of a Response message 550. The other part of the Response message 550 is a digital certificate 555 obtained from a well-known Trusted Authority 560 (e.g., system administrator, company security, etc.) in which its public key "PUTA" 565 is widely disseminated. The digital certificate 555 is the public key of the token ("PUT") 575 encrypted with the private key of the Trusted Authority "PRTA" 570. Both parts of the Response message 550 are transmitted to the security device 210.

Upon receiving the Response message 550, the security device 210 decrypts the digital certificate 555 with PUTA 565 to obtain PUT 575. Next, PUT 575 is used to decrypt RN_{prt} 545. Finally, RN 580 received from the token is compared to RN 540 transmitted to the token 120 and if these numbers are equivalent, the Response message 550 is correct.

Alternatively, in lieu of a password-based system being implemented within the node, the token may be configured to require a password or a personal identification number ("PIN"). Thus, the token remains in an inactive state unless its user periodically authenticates himself or herself. Of course, the advantage of having the password-based system employed within the node is that the node is already adapted with I/O devices (e.g., an alphanumeric keyboard) to assist a user in authenticating himself or herself. However, as stated previously, the node is susceptible to virus attacks which would not be an issue if the password-based system is employed within the token.

In this embodiment, the token requires periodic password or personal identification number ("PIN") authentication by the user so that if the token is lost or misplaced, it cannot be used by an unauthorized user once the token becomes inactive by failure to timely provide authentication information. It is plausible that the token may employ a type of biometric measurement device in lieu of a password-based system. For example, a thumbprint or fingerprint reader could be integrated into the token requiring the authorized user to periodically (e.g., sample at predetermined times or every hour, day, etc.) to ensure that the token itself cannot be used if it is lost. There are a few companies such as Digital Pathways and Security Dynamics that have developed tokens that require user authentication to operate. However, these tokens do not lend themselves to periodic authentication through Challenge and Response messages as illustrated above.

Referring now to Figure 7, the operations of the token implemented with a password-based system are illustrated below. First, in Step 600, at a periodic interval, the user provides authentication information to the token. If the authentication information is correct, the token is functional and exists in an active state (Steps 605-610). Thereafter, after a preselected period of time has elapsed, the token enters into an invalid state which requires the user to enter authentication information into the token again (Step 615). Otherwise, if the user authentication information is incorrect, the token remains nonfunctional (Step 615).

In the event that the token is in an active state, the token receives a query signal from the node once it is carried or worn within a predetermined distance from the node (Step 620). In that event, the token responds to the query with an identification message indicating the identity of the user (Step 625). Next, in Step 630, upon receiving the identification message from the token, the node generates and transmits a Challenge message directed to that token. Thereafter, the node awaits a Response message within a prescribed time period. If the node does not receive a Response message within that time or receives an incorrect Response message, access is denied to the node (Steps 635-645). However, if the node receives the Response message within the prescribed period of time and it is correct, the user is granted access to the node (Step 650).

Thereafter, timing circuitry within the node is set for the node to generate another Challenge message after a predetermined time period has expired (Step 655). Next, the token is checked to see whether it has been in the active state for longer than the selected time (Step 660). If so, the token becomes nonfunctional and the user is denied access to the node (Step 665). If the token is still active, the timing circuitry of the node is checked to see whether the predetermined time period has expired (Step 670). If not, the state of the token and expiration of the time period set by the timing circuitry in the node is checked at a later time. Otherwise, if the timing period has expired, the node is prompted to generate another Challenge message to the token for periodic authentication that the user is proximate to the node.

While various embodiments of the invention have been described, those skilled in the art will realize that other embodiments of the invention are easily foreseeable without departing from the spirit and scope of the present invention. For example, the token may initiate query messages to allow the node to determine when the token is in the proximity. Likewise, the periodic challenge/response communications may be initiated by the token rather than the node so long as the node still authenticates the token. Moreover, well known circuitry and operational steps are not set forth in detail in order to avoid unnecessarily obscuring the present invention. The invention should, therefore, be measured in terms of the following claims.

CLAIMS

What is claimed is:

1. A method to control an operating state of a node based on the proximity of an authorized user in possession of a token to the node, the method comprising the steps of:

(a) transferring a first message from the node to the token;

(b) transferring a second message from the token to the node, said second message being in response to the first message;

(c) determining whether the second message correctly responds to the first message, and placing the node in a first state if the second message correctly responds to the first message; and

(d) periodically performing steps (a) - (c) to ascertain whether the token is within a predetermined distance from the node, and

maintaining the node in the first state if the token correctly responds, and

placing the node in a second state if the token fails to respond or responds incorrectly.

2. The method according to claim 1, wherein said first state is an operational state and said second state is a non-operational state.

3. The method according to claim 2, wherein said node is a computer.

4. The method according to claim 2, wherein said node is a door control mechanism.

5. The method according to claim 1, wherein said first message includes a random number and said second message correctly responds to said first message by returning said random number.

6. The method according to claim 5, wherein said first message includes said random number in a non-encrypted format and said second message includes said random number encrypted with a private key associated with the token.

7. The method according to claim 5, wherein said first message includes said random number encrypted with a public key associated with the token and said second message includes said random number in a non-encrypted format.

8. The method according to claim 5, wherein said first message includes said random number and said second message includes said random number encrypted with a private key associated with the token and a digital certificate containing a public key associated with the token encrypted with a private key of a trusted authority.

9. The method according to claim 1, wherein said periodicity of said first and second message exchanges is programmable.

10. The method according to claim 1, wherein prior to step (a), the method comprises the steps of:

transferring a query message from the node to the token; and

transferring a response to the node by the token when the token is within said predetermined distance from the node.

11. The method according to claim 1, wherein prior to step (a), the method further comprises the steps of

transferring a query message from the token to the node; and

transferring a response message from the node to the token indicating that the node acknowledges that the token is within the predetermined distance.

12. A method to control an operating state of a node based on the proximity of an authorized user in possession of a token to the node, the method comprising the steps of:

(a) authenticating the token by exchanging messages between the token and the node;

(b) authenticating the node by exchanging at least a first and second messages between the token and the node and placing the node in a first state if said second message correctly responds to said first message; and

(c) periodically performing step (b) to ascertain whether the token is within a predetermined distance from the node, and

maintaining the node in the first state if the token correctly responds, and

placing the node in a second state if the token fails to respond or responds incorrectly.

13. The method according to claim 12, wherein prior to step (a), the method comprises the steps of:

transferring a query message from the node to the token; and

transferring a response to the node by the token when the token is within said predetermined distance from the node.

14. The method according to claim 12, wherein prior to step (c), the method further comprises the steps of

transferring query message from the token to the node; and

transferring a response message from the node to the token indicating that the node acknowledges that the token is within the predetermined distance.

15. A wireless authentication system to control an operating state of a first node having at least a first data bus to support communications internally within the first node based on the proximity of an authorized user possessing a token to the first node, the wireless authentication system comprising:

a security device implemented within the first node having a wireless transceiver, said security device generating a plurality of messages to be transmitted to the token through said wireless transceiver, wherein each of said plurality of messages is separately transmitted after a prescribed time interval has elapsed; and

the token that establishes a wireless communication link with said security device, wherein said security device and said token operate to place the first node in an operational state using said plurality of messages.

16. The wireless authentication system of claim 15, wherein each of said plurality of messages generated by said security device is separately transmitted after a prescribed time interval has elapsed.

17. The wireless authentication system according to claim 16, wherein the token (i) initially receives a first message of said plurality of messages, (ii) generates a message in response to said first message for transmission to said security device to place the first node in said operational state and (iii) generates a message in response to each of

said plurality of messages subsequent to said first message as long as the token remains within a predetermined distance from said security device.

18. The wireless authentication system according to claim 15, wherein said security device includes

a processing unit coupled to said first data bus, said processing unit generates each of said plurality of messages;

a memory unit coupled to said first data bus, said memory unit contains cryptographic information; and

an interface coupled to said first data bus, said interface receives each of said plurality of messages generated by said processing unit and transmits said plurality of messages to said token.

19. The wireless authentication system according to claim 18, wherein said security device further includes a random number generator coupled to said processing unit.

20. The wireless authentication system according to claim 18, wherein said token includes

a second data bus;

a wireless interface coupled to said second data bus, said second wireless interface is further coupled to said first wireless interface of said security device through a communication link to receive said plurality of messages and to transmit a corresponding plurality of messages in response to said plurality of messages;

a memory element coupled to said second data bus, said memory element contains cryptographic information; and

a processor coupled to said second data bus, said processor generates said corresponding plurality of messages in response to said plurality of messages.

21. The wireless authentication system according to claim 20, wherein said token further includes a power source to provide power to at least said memory element and said processor.

22. The wireless authentication system according to claim 17, wherein said first message includes a random number and said second message correctly responds to said first message by returning said random number.

23. The wireless authentication system according to claim 17, wherein said first message includes said random number in a non-encrypted format and said second message includes said random number encrypted with a private key associated with the token.

24. The wireless authentication system according to claim 17, wherein said first message includes said random number encrypted with a public key associated with the token and said second message includes said random number in a non-encrypted format.

25. The wireless authentication system according to claim 17, wherein said first message includes said random number and said second message includes said random number encrypted with a private key associated with the token and a digital certificate containing a public key associated with the token encrypted with a private key of a trusted authority.

26. The wireless authentication system according to claim 15, wherein the node is one of a computer and a door control mechanism.

27. A wireless authentication system to control an operating state of a first node based on the proximity of an authorized user to the

first node having a wireless transceiver means, the wireless authentication system comprising:

security means for generating a plurality of messages for transmission via the wireless transceiver means to a token means possessed by the authorized user, each of said plurality of messages is separately transmitted after a prescribed time interval has elapsed, said security means is implemented within the first node; and

said token means for initially receiving a first message of said plurality of messages, for generating a message in response to said first message for transmission to said security means to place the first node in an operational state and for generating a message in response to each of said plurality of messages subsequent to said first message as long as said token means remains within a predetermined distance from said security means.

28. The wireless authentication system according to claim 27, wherein said security means includes

first bus means for providing a data path within the first node;

first processor means for generating each of said plurality of messages, said first processor means being coupled to said first bus means;

first memory means for containing cryptographic information, said first memory means being coupled to said first bus means; and

first interface means for receiving each of said plurality of messages generated by said first processor means and for transmitting said plurality of messages to said token means, said first interface means is coupled to said first bus means and to a second interface means of said token through a wireless communication link therebetween.

29. The wireless authentication system according to claim 28, wherein said token means includes

second bus means for providing a data path within said token means;

said second interface means for receiving said plurality of messages and for transmitting a corresponding plurality of messages in response to said plurality of messages, said second interface means being coupled to said second bus means and to said first interface means of said security means through the communication link;

second memory means for storing cryptographic information, said second memory means being coupled to said second bus means; and

second processor means for generating said corresponding plurality of messages in response to said plurality of messages, said second processor means being coupled to said second bus means.

30. The wireless authentication system according to claim 29, wherein said token means further includes power means for providing power to at least said second memory means and said second processor means.

31. The wireless authentication system according to claim 27, wherein said first message includes a random number and said second message correctly responds to said first message by returning said random number.

32. The wireless authentication system according to claim 27, wherein said first message includes said random number in a non-encrypted format and said second message includes said random number encrypted with a private key associated with the token means.

33. The wireless authentication system according to claim 27, wherein said first message includes said random number encrypted with a public key associated with the token means and said second message includes said random number in a non-encrypted format.

34. The wireless authentication system according to claim 27, wherein said first message includes said random number and said second message includes said random number encrypted with a private key associated with the token means and a digital certificate containing a public key associated with the token means encrypted with a private key of a trusted authority.

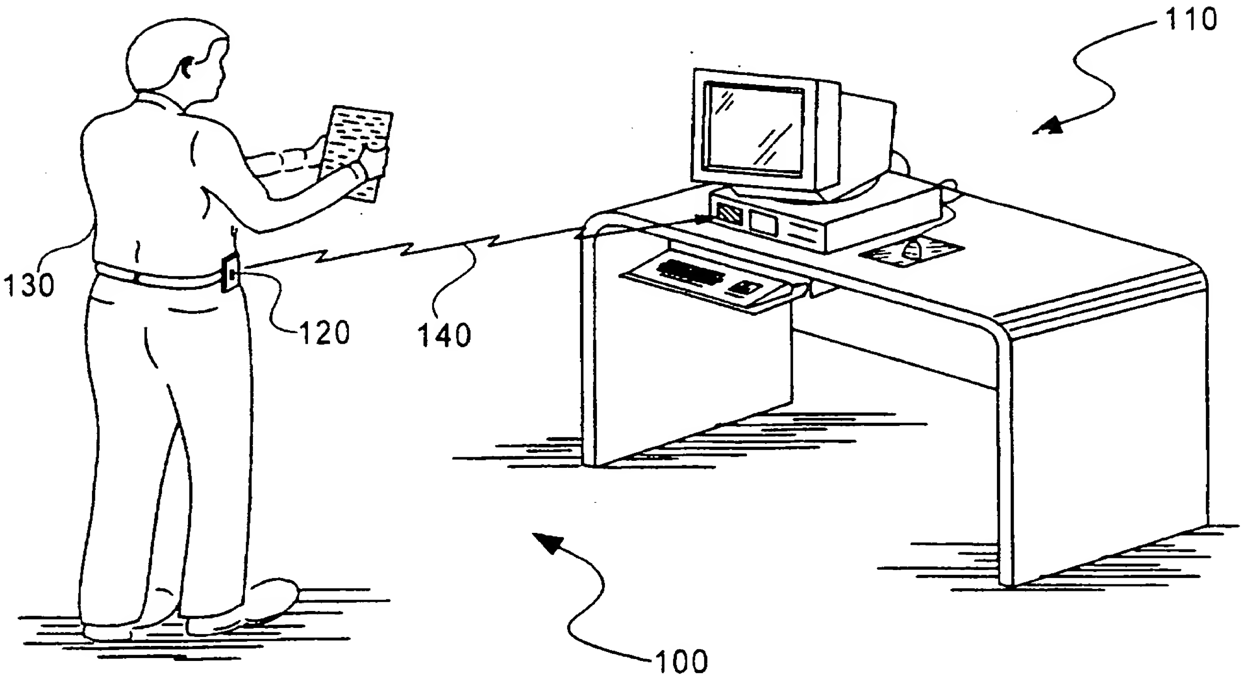


FIG. 1

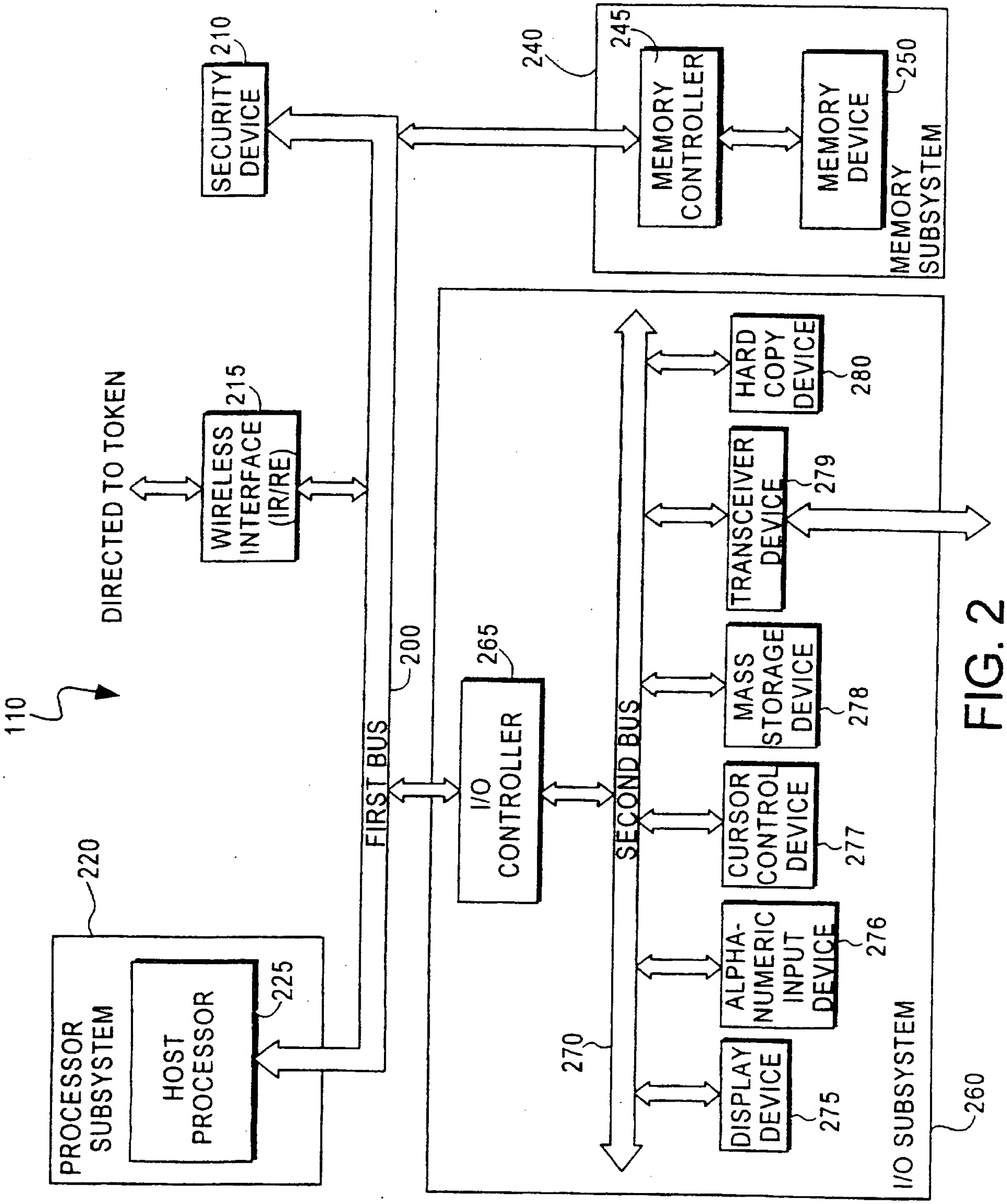

110
DIRECTED TO TOKEN
SECURITY DEVICE
210
WIRELESS INTERFACE (IR/RF)
215
MEMORY CONTROLLER
245
MEMORY DEVICE
250
240
MEMORY SUBSYSTEM
200
FIRST BUS
PROCESSOR SUBSYSTEM
220
HOST PROCESSOR
225
I/O CONTROLLER
265
SECOND BUS
270
HARD COPY DEVICE
280
TRANSCEIVER DEVICE
279
MASS STORAGE DEVICE
278
CURSOR CONTROL DEVICE
277
ALPHA-NUMERIC INPUT DEVICE
276
DISPLAY DEVICE
275
I/O SUBSYSTEM
260

FIG. 2

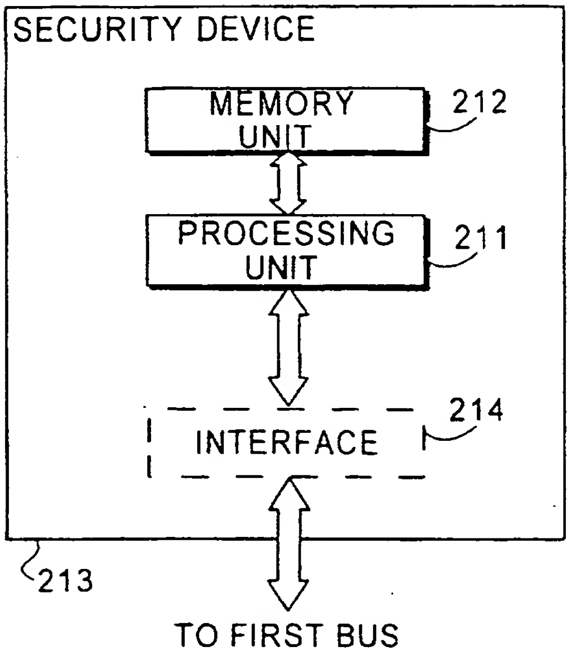

SECURITY DEVICE
MEMORY UNIT
212
PROCESSING UNIT
211
214
INTERFACE
213
TO FIRST BUS

FIG. 3

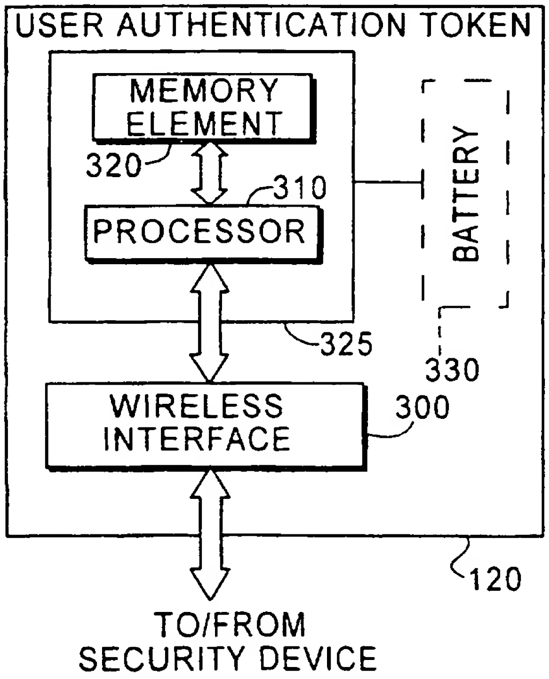

USER AUTHENTICATION TOKEN
MEMORY ELEMENT
320
310
PROCESSOR
BATTERY
325
330
WIRELESS INTERFACE
300
120
TO/FROM SECURITY DEVICE

FIG. 4

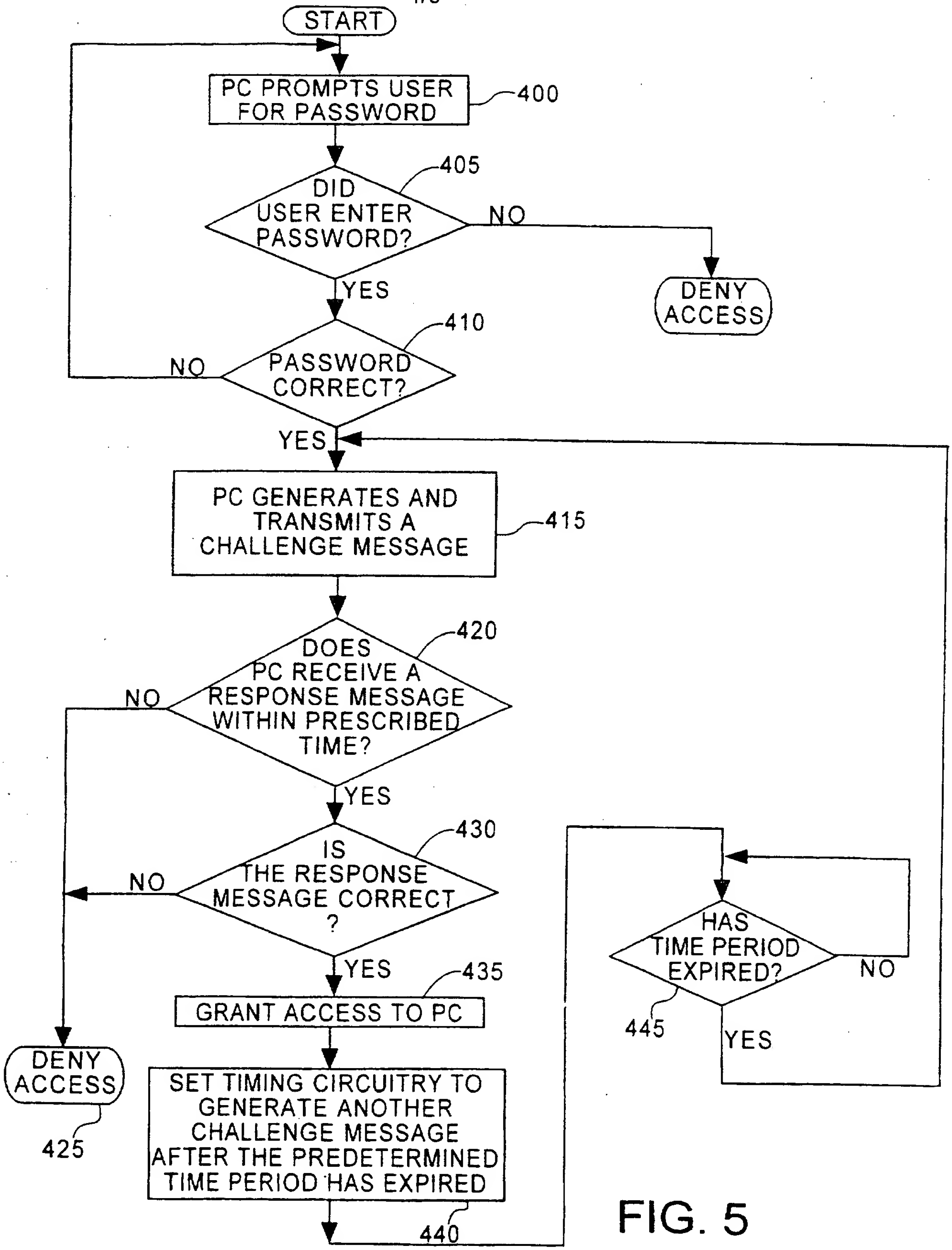

START
PC PROMPTS USER FOR PASSWORD
400
DID USER ENTER PASSWORD?
405
NO
DENY ACCESS
YES
PASSWORD CORRECT?
410
NO
YES
PC GENERATES AND TRANSMITS A CHALLENGE MESSAGE
415
DOES PC RECEIVE A RESPONSE MESSAGE WITHIN PRESCRIBED TIME?
420
NO
YES
IS THE RESPONSE MESSAGE CORRECT ?
430
NO
YES
GRANT ACCESS TO PC
435
DENY ACCESS
425
SET TIMING CIRCUITRY TO GENERATE ANOTHER CHALLENGE MESSAGE AFTER THE PREDETERMINED TIME PERIOD HAS EXPIRED
440
HAS TIME PERIOD EXPIRED?
445
NO
YES

FIG. 5

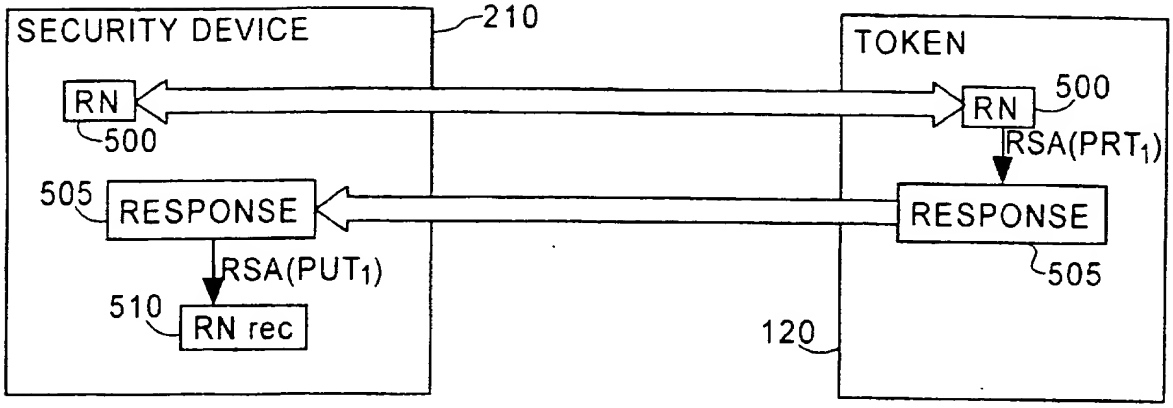

SECURITY DEVICE
210
TOKEN
RN
500
RN
500
RSA(PRT1)
505
RESPONSE
RESPONSE
505
RSA(PUT1)
510
RN rec
120

FIG. 6A

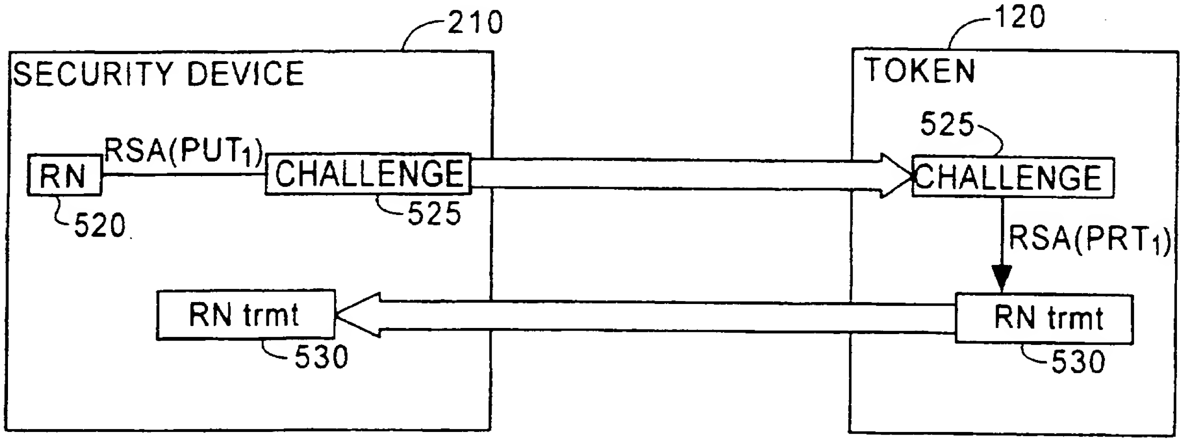

210
120
SECURITY DEVICE
TOKEN
525
RN
RSA(PUT1)
CHALLENGE
CHALLENGE
520
525
RSA(PRT1)
RN trmt
RN trmt
530
530

FIG. 6B

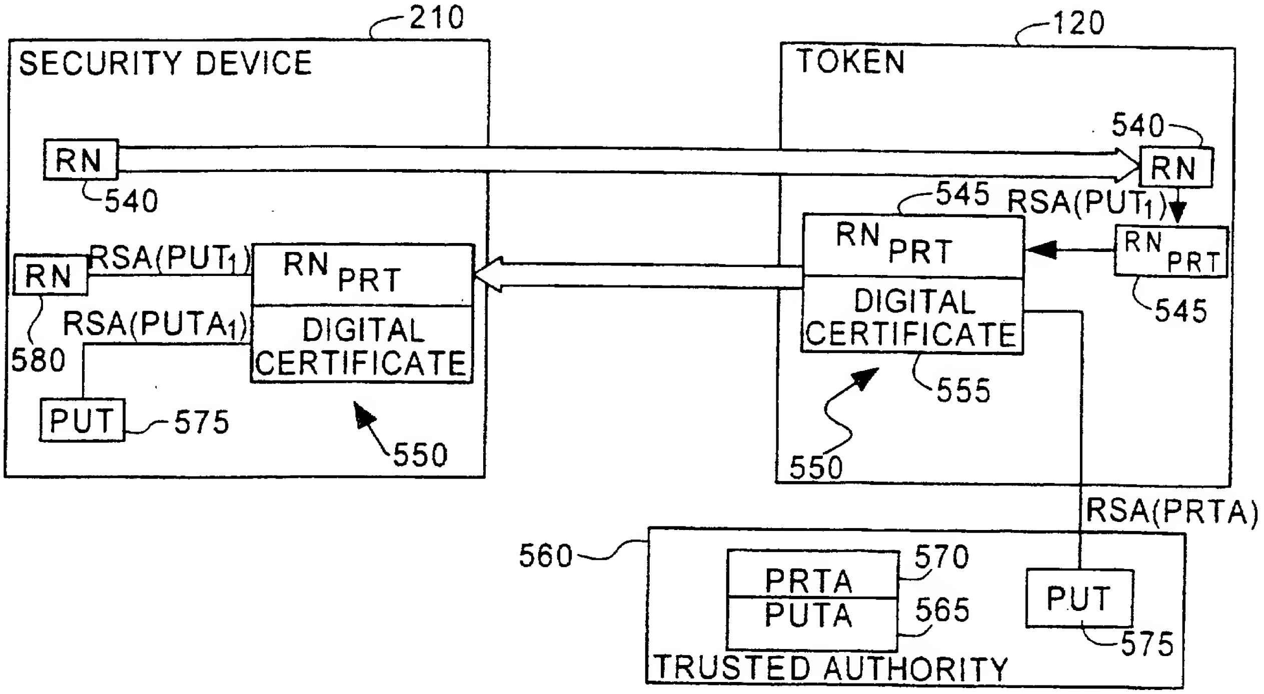

210
SECURITY DEVICE
RN
540
RN
RSA(PUT1)
RN PRT
RSA(PUTA1)
DIGITAL CERTIFICATE
580
PUT
575
550
120
TOKEN
540
RN
545
RSA(PUT1)
RN PRT
RN PRT
DIGITAL CERTIFICATE
545
555
550
RSA(PRTA)
560
570
PRTA
PUTA
565
PUT
575
TRUSTED AUTHORITY

FIG. 6C

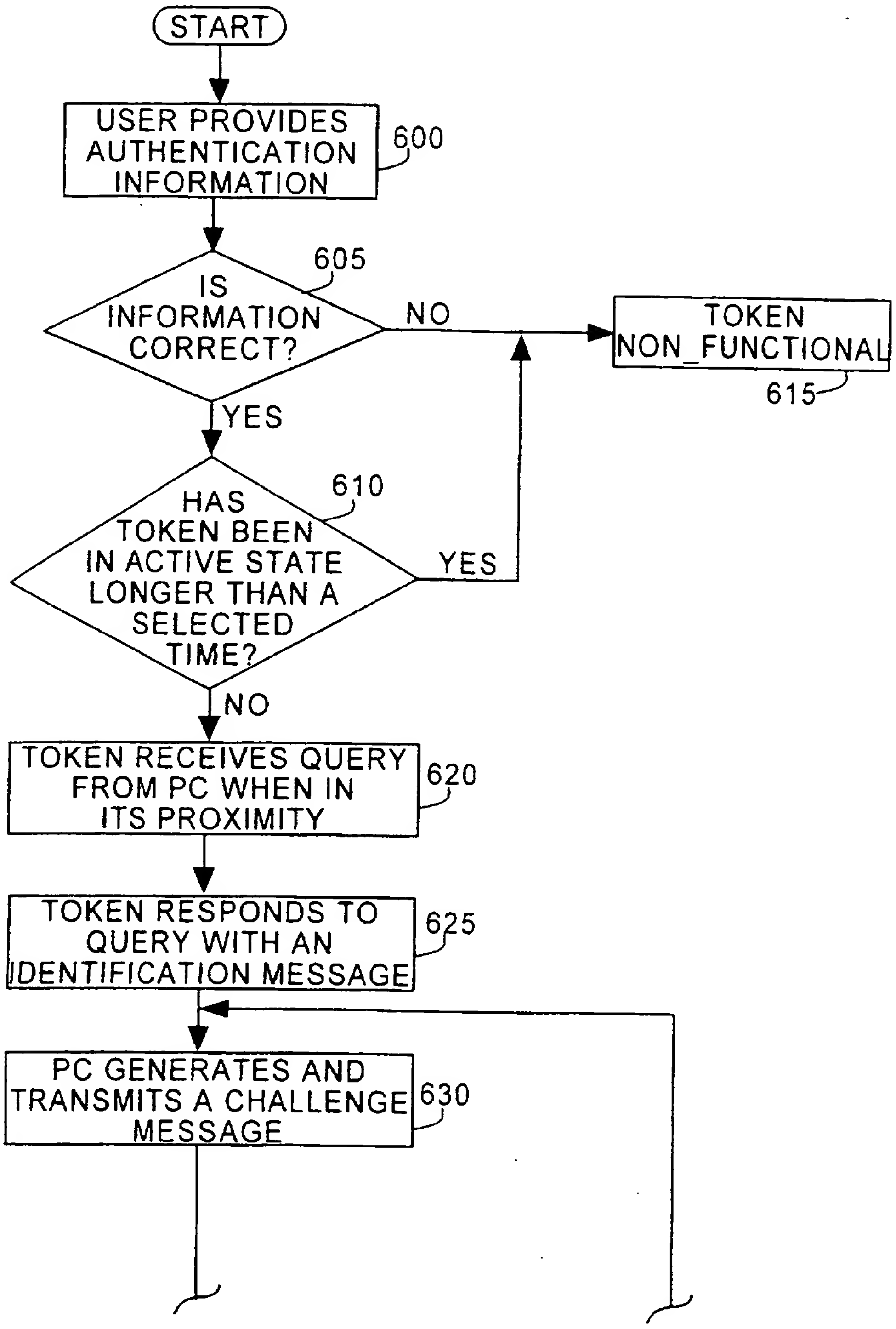

START
USER PROVIDES AUTHENTICATION INFORMATION
600
IS INFORMATION CORRECT?
605
NO
TOKEN NON_FUNCTIONAL
615
YES
HAS TOKEN BEEN IN ACTIVE STATE LONGER THAN A SELECTED TIME?
610
YES
NO
TOKEN RECEIVES QUERY FROM PC WHEN IN ITS PROXIMITY
620
TOKEN RESPONDS TO QUERY WITH AN IDENTIFICATION MESSAGE
625
PC GENERATES AND TRANSMITS A CHALLENGE MESSAGE
630

FIG. 7A

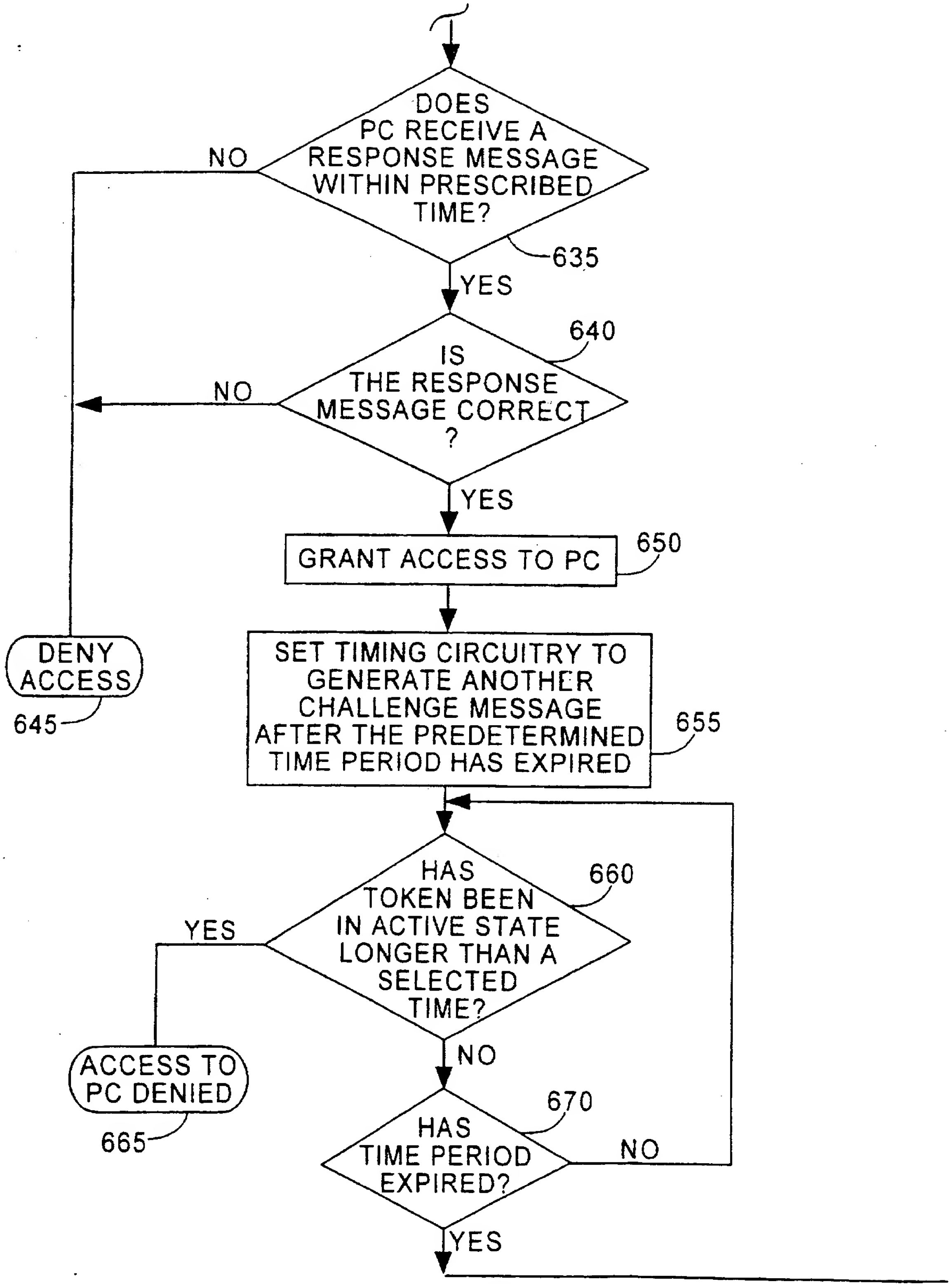

DOES PC RECEIVE A RESPONSE MESSAGE WITHIN PRESCRIBED TIME?
635
NO
YES
IS THE RESPONSE MESSAGE CORRECT ?
640
NO
YES
GRANT ACCESS TO PC
650
DENY ACCESS
645
SET TIMING CIRCUITRY TO GENERATE ANOTHER CHALLENGE MESSAGE AFTER THE PREDETERMINED TIME PERIOD HAS EXPIRED
655
HAS TOKEN BEEN IN ACTIVE STATE LONGER THAN A SELECTED TIME?
660
YES
NO
ACCESS TO PC DENIED
665
HAS TIME PERIOD EXPIRED?
670
NO
YES

FIG. 7B

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/04025

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :H04L 9/32;
US CL : 380//23, 25; 340/825.31
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380//23, 25; 340/825.31

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS: search terms-authenticate, transponder, periodic, random number, certificate

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,097,505 A (WEISS) 17 March 1992, column 2, lines 38-53; column 3, lines 58-61; column 7, lines 6-16; column 9, lines 51-67.	1-4, 9-18, 20-30
Y	US 5,144,667 A (POGUE, JR. ET AL) 01 September 1992, column 5, lines 9-30; column 3, line 58- column 4, line 39.	5-7, 22-24, 32, 33
X	US 5,131,038 A (PUHL ET AL) 14 July 1992, column 4, lines 5-24.	1-4, 9-18, 20, 26-29
A	US 5,432,851 A (SCHEIDT ET AL) 11 July 1995, column 3, lines 22-50.	1, 12, 15, 27
A	US 5,280,527 A (GULLMAN ET AL) 18 January 1994, column 2, lines 30-39.	1, 12, 15, 27

☒ Further documents are listed in the continuation of Box C. □ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search 11 JUNE 1997	Date of mailing of the international search report 11 JUL 1997
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer GILBERTO BARRÓN Telephone No. (703) 306-4177

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/04025

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,377,269 (HEPTIG ET AL) 27 December 1994, column 3, lines 11-24.	1, 12, 15, 27